

11. November 2006

VPN Zugang

**Netzstufe I
Schulen ans Internet, Kt. Bern
Funktionsweise und
technische
Voraussetzungen**

**Markus Marcin
Haotung Dam**

Inhalt

1	Ausgangslage	3
1.1	Virtual Private Network	3
1.2	VPN-RAS Zugang Schulen ans Netz	3
2	Funktionsweise	5
2.1	RAS-Account beantragen	5
2.2	VPN-Zugang einrichten: VPN-Client, Profil, Benutzer und Passwort	5
2.3	Überprüfen der Funktionstüchtigkeit des Internetanschlusses	7
2.4	Remote Zugriff auf Server an der Schule	8
2.5	Voraussetzungen für den Remotezugriff	10
3	Anhang	14
3.1	Bsp. Konfigurationsblatt Schule Netzstufe 1	14
3.2	Netzwerkkonzept Schulen ans Internet mit VPN-Zugang	15

1 Ausgangslage

1.1 Virtual Private Network

Virtual Private Network (VPN) (dt.: Virtuelles Privates Netz) ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netz (zum Beispiel das Internet) nutzt. Teilnehmer eines VPN können Daten wie in einem internen LAN austauschen. Die einzelnen Teilnehmer selbst müssen hierzu nicht direkt verbunden sein. Die Verbindung über das öffentliche Netz wird üblicherweise verschlüsselt. Der Begriff „Private“ impliziert jedoch nicht, wie vielfach angenommen, dass es sich um eine verschlüsselte Übertragung handelt. Eine Verbindung der Netze wird über einen Tunnel zwischen VPN-Client und VPN-Server (Concentrator) ermöglicht. Meist wird der Tunnel dabei gesichert, aber auch ein ungesicherter Klartexttunnel ist ein VPN.

1.2 VPN-RAS Zugang Schulen ans Internet

Allgemein

Swisscom bietet den Systemadministratoren der Netzstufe 1 die Möglichkeit die Serverinfrastruktur an den Schulen über einen Remote-Zugang zu warten.

Die folgenden Abbildungen zeigen, wie ein Netz an der Schule aufgebaut sein muss, damit ein Zugriff auf die Serverinfrastruktur möglich wird.

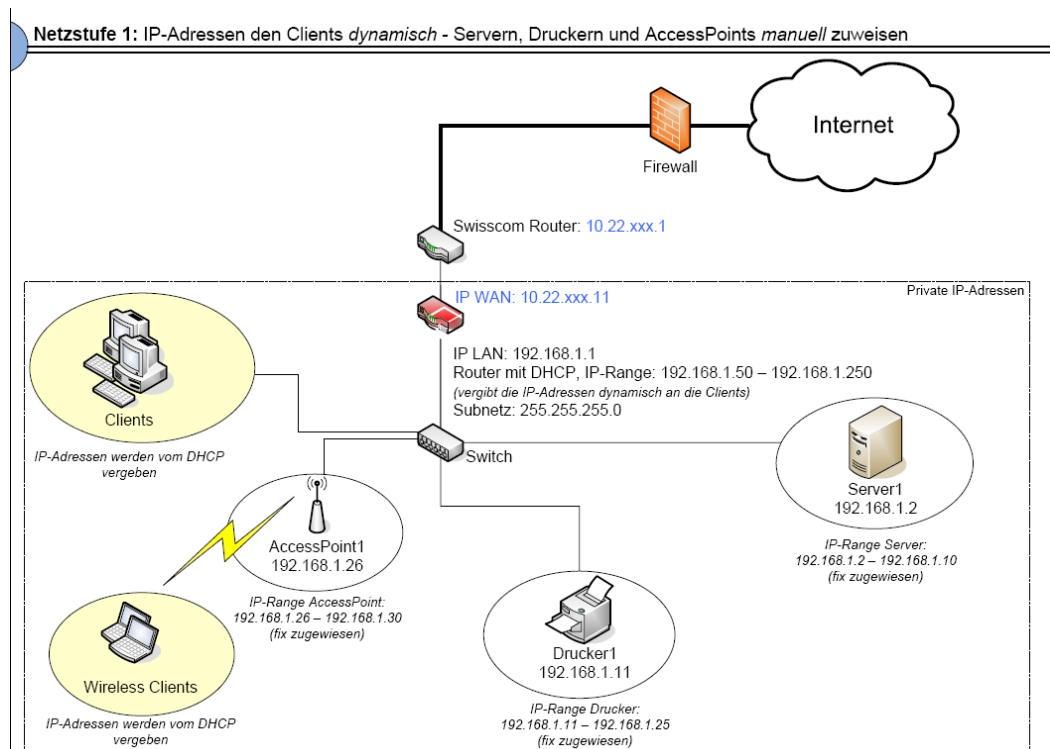


Abbildung 1: Aufbau des Netzwerkes ohne VPN-Zugang

Wie Sie in der Abbildung 2 erkennen können, sind im bestehenden Netzwerk der Schule (Abb.1) nur geringfügige Anpassungen für den VPN-Zugriff notwendig (vgl. Abb1. mit Abb2.).

Die Schulinformatik empfiehlt den Schulen zwischen dem Router der Swisscom und dem Router der Schule einen kleinen Switch zu platzieren. Vom Switch wird ein Netzkabel zum Server geführt, welcher ferngewartet werden soll. Der Server muss eine IP-Adresse aus dem Range der Swisscom (siehe Konfigurationsblatt, Anschluss Schulen ans Internet) aufweisen, z. B. 10.21.62.193. (Testserver Schulinformatik Oberstufe Hochfeld Bern).

Verwendungszweck

Mit Hilfe des RAS-Zugangs der Swisscom können Sie von zu Hause aus feststellen, ob der Router der Swisscom in Ihrer Schule funktioniert. Für die Analyse bei Störungen des Anschlusses von Schulen ans Internet ist der RAS-VPN-Zugang eine wichtige Lösung (s. Kap. 2.3)

Daneben können Sie aber auch mit Hilfe von Fernwartungstools auf Server an der Schule zugreifen (s. Kap. 2.4).

Die Kommunikation zwischen den Rechnern über die VPN-Verbindung wird verschlüsselt. Diese Sicherheitsvorkehrungen genügen den heute bekannten Anforderungen.

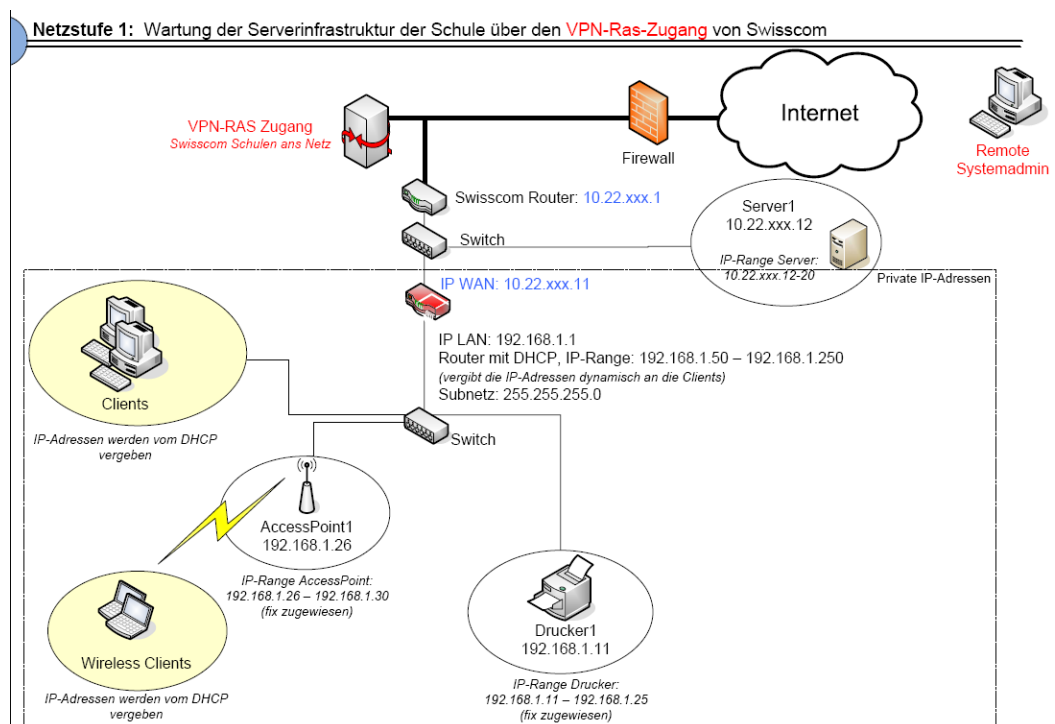


Abbildung 2: Aufbau Netzwerk Schule für die Wartung über den VPN-Ras Zugang Swisscom

2 Funktionsweise

2.1 RAS-Account beantragen

Die ICT-Verantwortlichen an den Schulen können bei der Koordinationsstelle von Schulen ans Internet des Kantons Bern einen VPN-RAS Zugang beantragen.

- **Für die Schulen der Netzstufe 1 wird pro Schule nur ein VPN-Zugang eingerichtet.**
- **Die Schulen verpflichten sich diesen VPN-RAS Zugang ausschliesslich für die Wartung von ICT-Infrastruktur (z. B. Schulserver) zu nutzen. Die Schule übernimmt die Verantwortung für Missbräuche mit dem VPN-Zugang.**

2.2 VPN-Zugang einrichten: VPN-Client, Profil, Benutzer und Passwort

Sobald der Antrag bewilligt ist, erhält die Schule von der Koordinationsstelle den Link für den Download des VPN-Clients und ein entsprechendes Benutzerprofil per E-Mail. Den Benutzernamen und das Kennwort für die VPN-Verbindung erhalten die Antragstellenden aus Sicherheitsgründen mit der Briefpost.

Den Cisco-VPN-Client einrichten:

Nach der Installation des VPN-Clients muss der Systemadministrator das VPN-Profil des Schulen ans Internet Zugangs (.pcf File) im Client importieren (s. Abb. 4 und 5). Anschliessend kann eine Verbindung zum VPN-Gateway von Schulen ans Internet aufgebaut werden (s. Abb. 2).

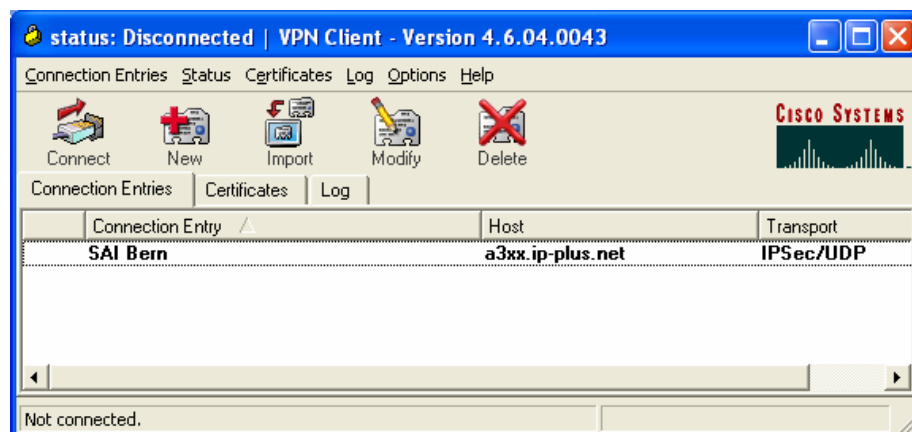


Abb. 4 Cisco VPN-Client und User-Profile SAI Bern

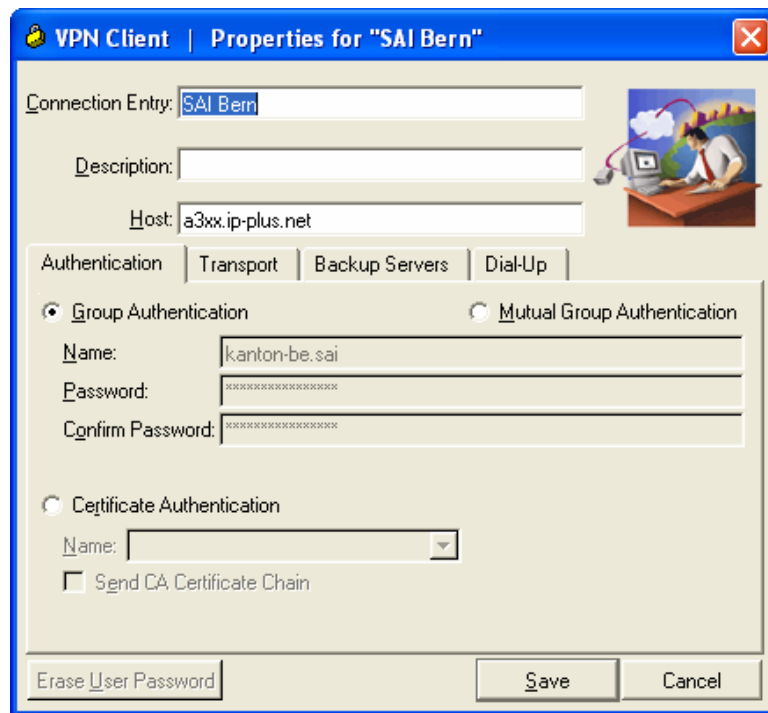


Abb. 5 User Profile SAI Bern

Beim Drücken der Schaltfläche „Connect/Verbinden“ wird der User aufgefordert Benutzernamen und Passwort einzugeben z. B. vorname.nachname@kanton-be.sai
Password: ***** (s. Abb. 6).



Abb. 6 Benutzer Authentifizierung am VPN-Gateway der Swisscom

Ist der Verbindungsaufbau erfolgreich, können die Netzwerkeinstellungen überprüft werden. Das Gerät erhält über die VPN-Verbindung automatisch eine IP-Adresse aus dem Bereich von Schulen ans Internet. Obschon von zu Hause über den Internet Service Provider (ISP) eine Verbindung via Internet ins Schulnetz hergestellt wird, erhalten Sie eine Netzwerkadresse aus dem Bereich des Schulnetzes (s. Abb. 7 und 8).

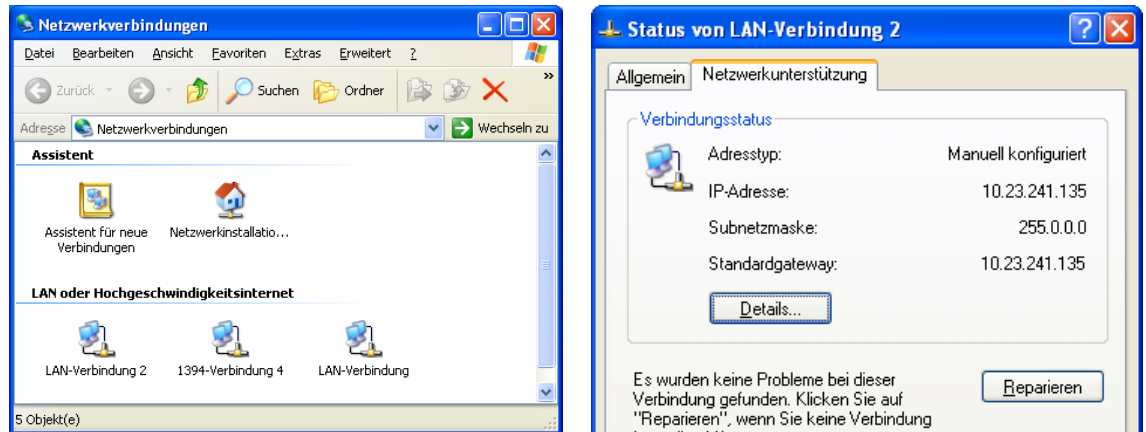


Abbildung 7/8 IP-Adressen am virtuellen Netzwerkadapter „LAN-Verbindung-2“

2.3 Überprüfen der Funktionstüchtigkeit des Internetanschlusses

Sie können mit Netzwerktools einen „Ping“ absetzen und überprüfen, ob der Router der Swisscom an Ihrer Schule von Aussen erreichbar ist. So lässt sich bei Störungen des Internetanschlusses leicht feststellen, ob das Problem der Störung intern oder extern gesucht werden muss. Ist der Router der Swisscom von Aussen erreichbar, so liegt mit hoher Wahrscheinlichkeit eine Störung im Netzwerk der Schule vor. Ist der Router der Swisscom von Aussen nicht erreichbar, kann der Systemverantwortliche von einer Störung im Netzwerk der Swisscom ausgehen.

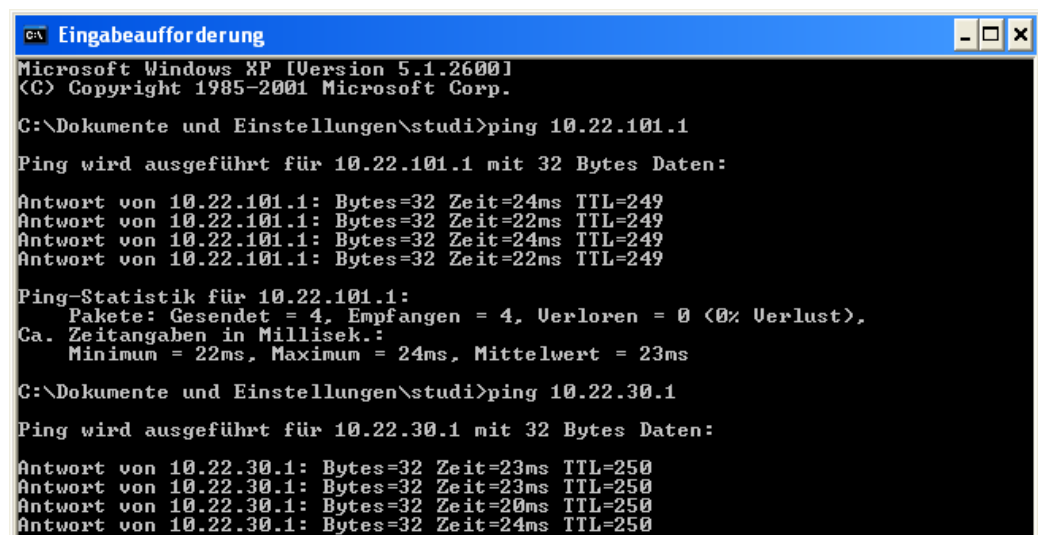


Abbildung 9 Erreichbarkeit des Routers der Swisscom an der Schule überprüfen
„ping 10.22.101.1 oder 10.22.30.1“

2.4 Remote Zugriff auf Server an der Schule



Abbildung 10 Eine Remotedesktopverbindung herstellen



Abbildung 11 Standort des Testserver der Schulinformatik an der Oberstufe Hochfeld in Bern

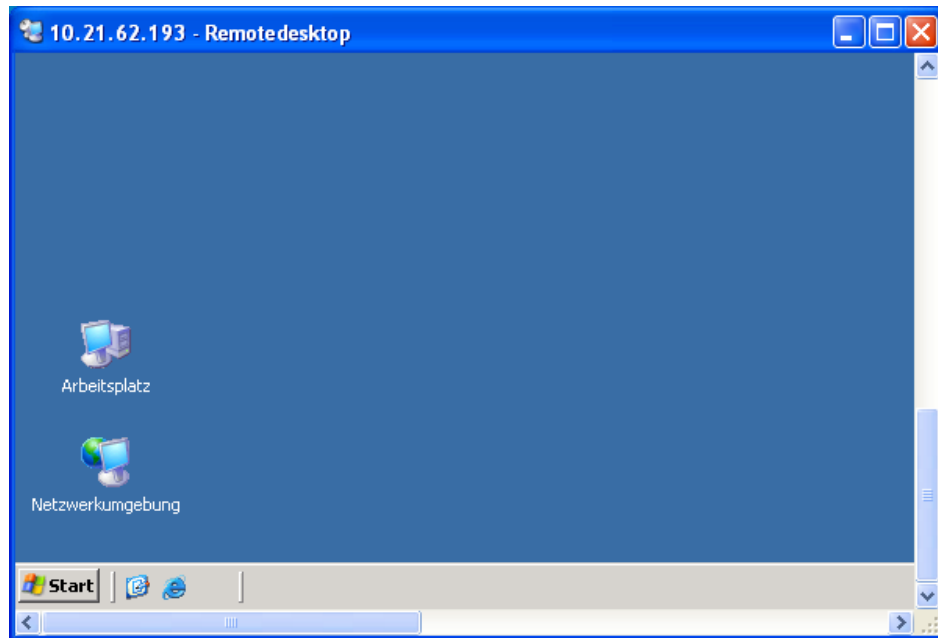


Abbildung 12 Remotdesktop des Testservers der Schulinformatik
an der Oberstufe Hochfeld in Bern

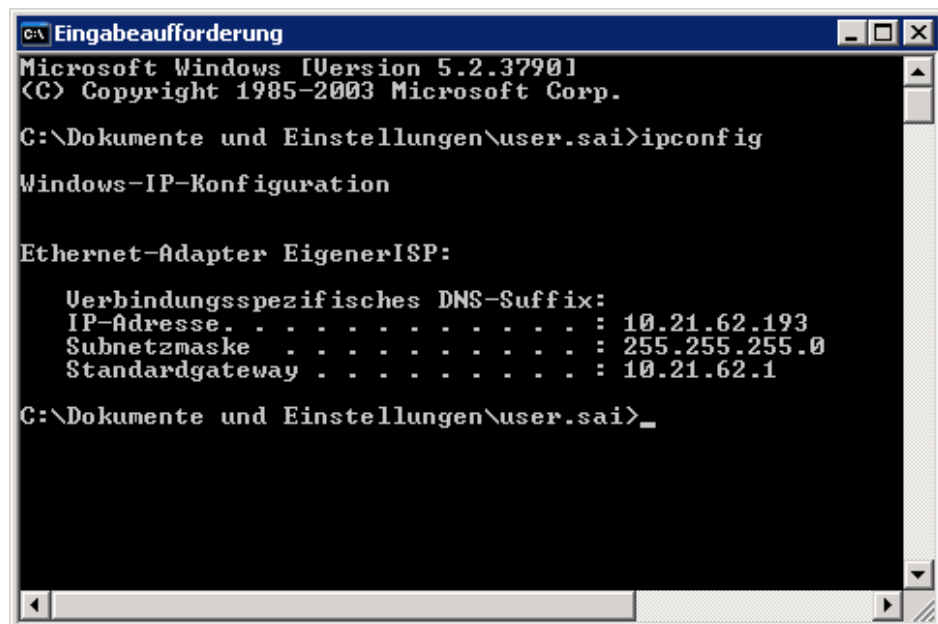


Abbildung 13 IP Adresse Testserver Schulinformatik

2.5 Voraussetzungen für den Remotezugriff

Das Windows Serverbetriebssystem verfügt standardmässig über Fernwartungsmöglichkeiten. Dazu muss einzig „Remotedesktop“ auf dem Server aktiviert werden (s. Abb. 14).

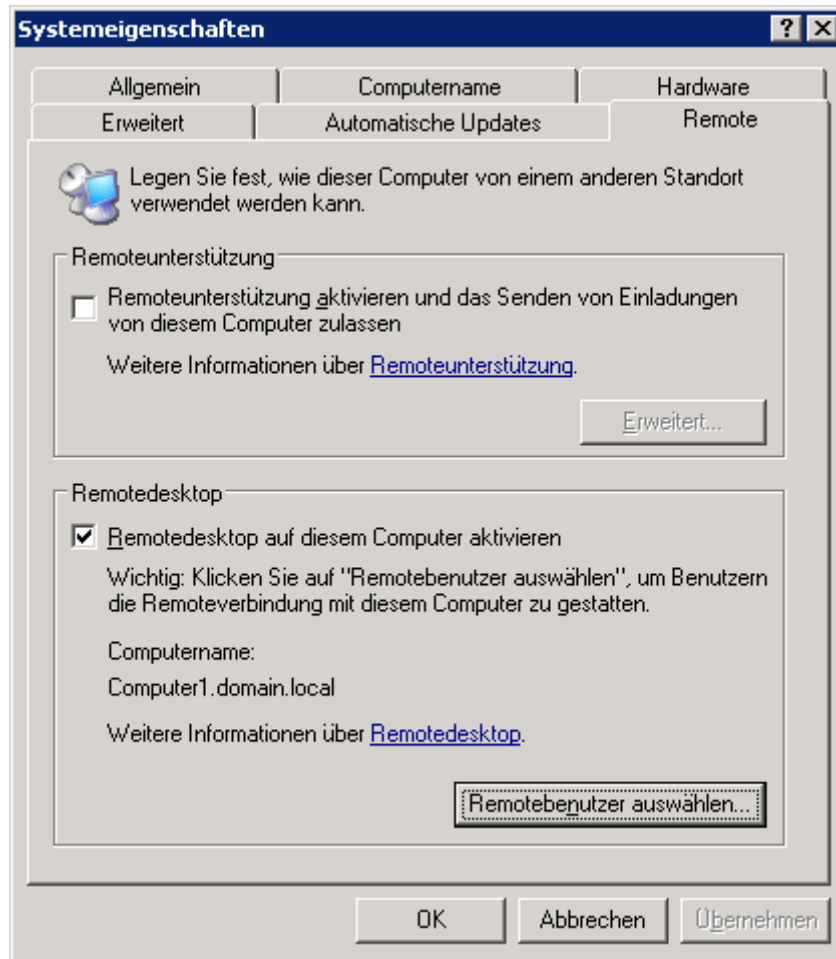


Abbildung 14 Remotedesktop aktivieren

3 Sicherheitsvorkehrungen

3.1 User für Remotezugriff definieren

Aus Sicherheitsgründen ist es sinnvoll den Remote-Zugriff nur ganz bestimmten Benutzern zu ermöglichen. Auf den Testserver der Schulinformatik kann einzig der User „user.sai“ zugreifen (s. Abb. 15).

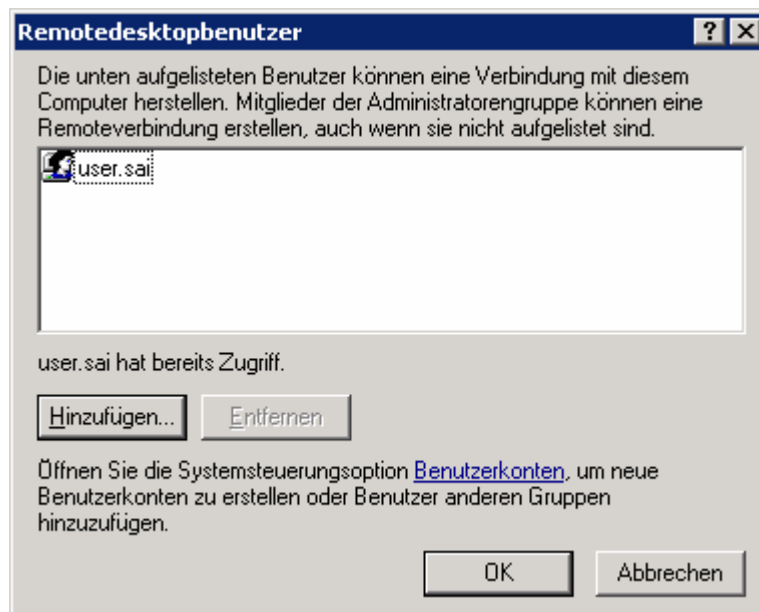


Abbildung 15 Benutzer für den Zugriff auf Remotedesktop definieren

3.2 Computer für Remotezugriff definieren

Festlegen (z. B. mit Hilfe der Einstellungen der Firewall), welche Computer auf den Server zugreifen dürfen.

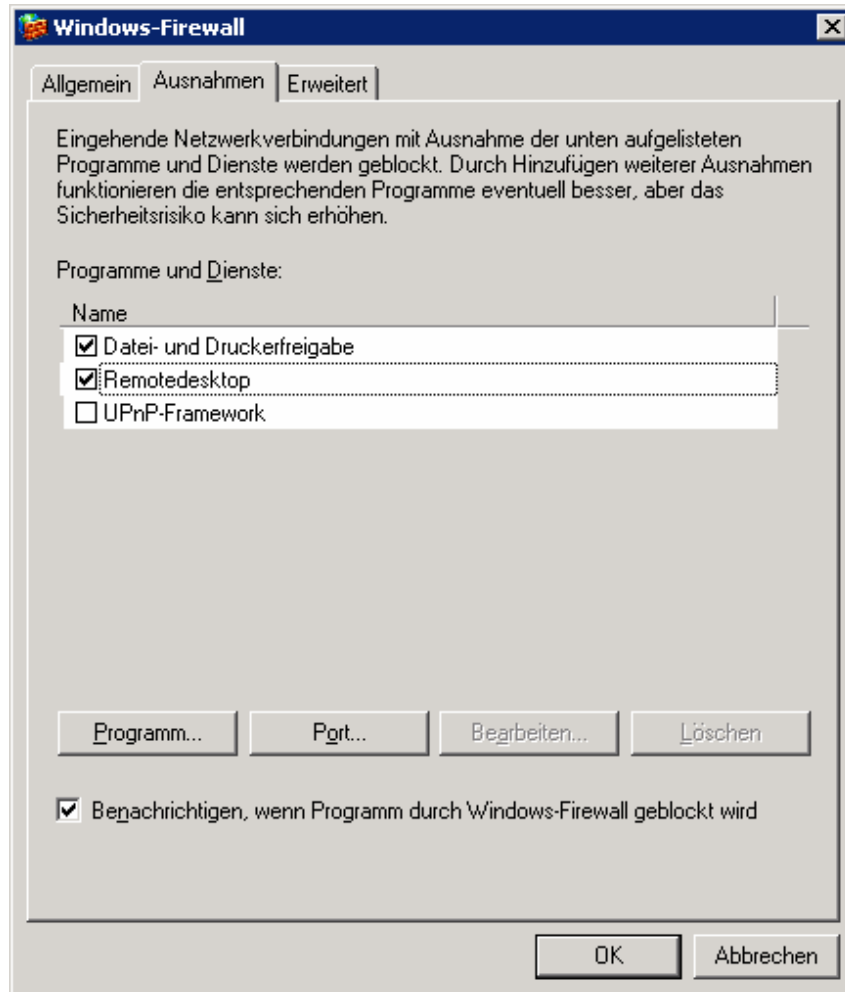


Abb.16 Einstellungen Firewall z. B. Windows 2003 Server

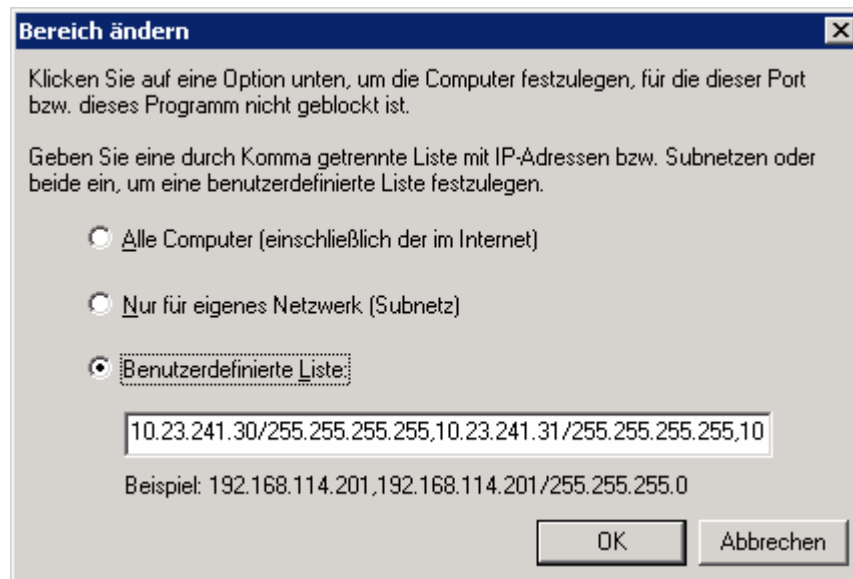


Abb. 17 zeigt die Geräte, welche von der Firewall beim Remote-Zugriff nicht geblockt werden

4 Anhang

4.1 Bsp. Konfigurationsblatt Schule Netzstufe 1

IP-Adressierung allgemein

Jeder Computer, der sich mit dem Internet verbindet, benötigt grundsätzlich eine eindeutige Identifikationsadresse (die so genannte IP-Adresse).

Jede Schule, die zum Bildungsnetz des Kantons Bern verbunden wird, erhält daher einen eigenen dafür vorgesehenen Adressbereich.

Der IP-Range für:

Primarschule Muster, Bernost, 37366 Bultigen (Routerlabel **ip-knbe-ch-rxb-r-002**) lautet
10.22.124.x

Wie die IP-Adressen auf die Clients verteilt werden, ist der Schule überlassen.

Die Schulinformatik empfiehlt Ihnen, den Computern im lokalen Netzwerk die IP-Adressen mit einem DHCP-Dienst **dynamisch** zuzuweisen. Am einfachsten lässt sich dies mit einem zusätzlichen Router bewerkstelligen. Der Router der Swisscom beinhaltet keine solche Funktion.

Adressvergabe (IP-Adressen)

IP-Adresse	10.22.124.1	ist reserviert für den Router (Gateway) der Swisscom
IP-Adressen	10.22.124.2 - 10.22.124.10	sind reserviert für Swisscom Dienste
IP-Adressen	10.22.124.11 - 10.22.124.254	können für die Geräte der Schule nach eigenem Gutdünken verwendet werden
Subnet Mask	255.255.255.0	
Default Gateway	10.22.124.1	

DNS-Server

Wenn in Ihrem Netzwerk kein DNS-Server in Betrieb ist, müssen die DNS-Server des Bildungsnetzes benutzt werden.

DNS1	164.128.36.36
DNS2	164.128.36.37

4.2 Netzwerkkonzept Schulen ans Internet mit VPN-Zugang

